REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 1, 12-14 AND 16-18 UNDER 35 U.S.C. § 102

Claims 1, 12-14 and 16-18 stand rejected as being anticipated by the Aura patent (United States Patent No. 6,711,400, issued March 23, 2004, hereinafter "Aura"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Aura fails to disclose or suggest the novel invention of encrypting a message to be sent including an expected nonce value and a new nonce value, where the expected nonce value and the new nonce value are both recoverable from the message using only knowledge possessed by the message recipient prior to receipt of the message, as claimed in Applicants' independent claim 1, 13, 16 and 18.

In contrast, Aura teaches that a recipient of a message (*i.e.*, a mobile station) requires at least two new pieces of information (*i.e.*, a new random number value, RAND2, and a specially generated key, SRES1) generated by the message's sender (*i.e.*, an authentication centre) in order to extract information from the message. That is, the sending party generates the special key (using a plurality of one-way hash functions) and a new random number and sends both to the recipient, who already is in possession of a first random number (*i.e.*, RAND1) and a shared cipher key (Ki). The first random number, the second random number and the cipher key are all required to extract any information from the message (see, *e.g.*, Aura at column 7, lines: "The network ... sends the values RAND2 and SRES1 [received from the authentication centre] to the mobile station ... The mobile station receives the values RAND2 and SRES. Additionally, it has the random number RAND1 ... and ... the cipher key Ki .... It enters these data ... to the algorithm ...").

Accordingly, if the key SRES1 can be equated with the encrypted message

claimed by the Applicants, as the Examiner suggests, then it is impossible for the recipient of the message to extract anything from the message without some additional information (*i.e.*, second random number RAND2). Without this additional information, the recipient can do nothing with the message. Thus, the recipient requires a combination of existing knowledge and new information provided by the sender in order to be able to extract information (*e.g.*, nonce values, or any other sort of information) from the message.

Moreover, the Applicants submit that the key SRES1, as taught by Aura, is not equivalent to the encrypted message claimed by the Applicants. As recited in the Applicants' claims, the encrypted message includes three main components: a message to be sent between two nodes in a network, an expected nonce value and a new nonce value. The presence of the nonce values (specifically the expected nonce) allows the recipient of the encrypted message to verify that the message included in the encrypted message is a legitimate communication (and not, for example, part of a replay attack on the network). The SRES 1 key taught by Aura, by contrast, contains no such message between sender and recipient and is simply a value that authenticates a network user.

Notably, the Applicants' invention positively claims the novel method of encrypting a message to be sent including an expected nonce value and a new nonce value, where the expected nonce value and the new nonce value are both recoverable from the message using only knowledge possessed by the message recipient prior to receipt of the message, as positively claimed by the Applicants. Aura clearly fails to disclose or suggest all of these limitations, as claimed in Applicants' independent claims 1, 13, 16 and 18. Specifically, Applicants' independent claims 1, 13, 16 and 18 recite:

> 1. A secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender node and the recipient node sharing a secret encryption key and an expected nonce value comprising:
>
> generating a new nonce value known to the sender node;
>
> encrypting the message, the expected nonce value and the new nonce value, using the encryption key, to create an encrypted message;
>
> transmitting the encrypted message from the sender node to the

recipient node; and

verifying, by the recipient node, that the encrypted message includes the expected nonce value, where the expected nonce value and the new nonce value are recoverable from the encrypted message using only knowledge possessed by the recipient node prior to receipt of the encrypted message. (Emphasis added)

13. A system for managing communications within a network collaboration group, comprising:

means for generating a new nonce value;

means for incorporating a message, an expected nonce value and the new nonce value in an encrypted message;

means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and

means for verifying, by the recipient node, that the encrypted message includes the expected nonce value, where the expected nonce value and the new nonce value are recoverable from the encrypted message using only knowledge possessed by the recipient node prior to receipt of the encrypted message. (Emphasis added)

16. A data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master node and the member node, the signal comprising:

the information to be transmitted;

an expected nonce value known to the master node and the member node; and

a new nonce value, different than the expected nonce, provided by a sender of the signal, the sender being one of the master node and the member node, where the expected nonce value and the new nonce value are recoverable from the signal using only knowledge possessed by the recipient node prior to encryption of the signal, the recipient node being one of the master node and the member node that did not send the signal. (Emphasis added)

> 18. A method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:
>
> encrypting-messages using a key shared by the master node and the member node, so as to protect confidentiality of the message; and
>
> embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages, where said plurality of updated nonce values are recoverable from the messages using only knowledge possessed by the recipient node prior to said encrypting, said recipient node being one of the master node and the member node that receives the encrypted messages. (Emphasis added)

The Applicants' invention is directed to methods and protocols for intrusion-tolerant management of collaborative network groups. As global users continue their migration to online network environments, the problem of vulnerability to malicious attacks (*e.g.*, by unauthorized users or "hackers") becomes more severe. Correspondingly, the need for "private" online groups that are resistant to intrusion by unauthorized users increases. Many known methods for providing private, secure communication channels for authorized users (such as virtual private networks or VPNs) remain vulnerable to unauthorized intrusions such as replay attacks (illegitimate interception, copying and re-transmission of legitimate, encrypted traffic). To preserve system integrity and availability, it is important that such attacks be recognized as illegitimate communications.

The Applicants' invention provides a means for transmitting a message from sender to recipient in an intrusion-tolerant manner. Communications between sender and recipient are encrypted with a cryptographic key known by both parties and include two nonce values in addition to the message. The first nonce value is an expected nonce value, already known to the receiver, while the second nonce value is a new nonce value generated by the sender. When the receiver receives the encrypted message, the receiver verifies, using the cryptographic key, that the message includes the expected nonce value. The presence of the expected nonce value confirms that the message is a legitimate message from the sender and is not part of an attack by an unauthorized party. The new nonce value then becomes the expected nonce value for

a subsequent message (*e.g.*, from receiver to sender).

As discussed above, Aura fails to teach or suggest a method in which an expected nonce value and a new nonce value are both recoverable from an encrypted message using only knowledge possessed by the message recipient prior to receipt of the message, as claimed in Applicants' independent claims 1, 13, 16 and 18. Therefore, the Applicants submit that independent claims 1, 13, 16 and 18 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 12, 14 and 17 depend from claims 1, 13 and 16 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 12, 14 and 17 are not anticipated by the teachings of Aura. Therefore, the Applicants submit that dependent claims 12, 14 and 17 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

II. REJECTION OF CLAIMS 2-11 AND 15 UNDER 35 U.S.C. § 103

Claims 2-11 and 15 stand rejected as being made obvious by Aura in view of the Janson et al. patent (United States Patent No. 5,729,608, issued March 17, 1998, hereinafter "Janson"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Janson, like Aura fails to disclose or suggest the novel method encrypting a message to be sent including an expected nonce value and a new nonce value, where the expected nonce value and the new nonce value are both recoverable from the message using only knowledge possessed by the message recipient prior to receipt of the message, as positively claimed by the Applicants. Janson thus fails to bridge the gap in the teachings of Aura. Therefore, the Applicants respectfully submit that independent claims 1 and 13 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-11 and 15 depend, respectively, from claims 1 and 13 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2-11 and 15 are not made obvious by the teachings of Aura in view of Janson. Therefore, the Applicants submit that dependent claims 2-11 and 15 also fully satisfy the requirements of 35 U.S.C. §103 and are

patentable thereunder.

III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

3/13/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702